QUESTION 61
When configuring NAT, the Internet interface is considered to be what?

A. local
B. inside
C. global
D. outside

Answer: D
Explanation:
Network address translation or NAT requires the Internet to be considered as an outside interface else it won't serve the purpose it intends to.

QUESTION 62
The ip helper-address command does what?

A. assigns an IP address to a host
B. resolves an IP address from a DNS server
C. relays a DHCP request across networks
D. resolves an IP address overlapping issue

Answer: C
Explanation:
When the DHCP client sends the DHCP request packet, it doesn't have an IP address. So it uses the all-zeroes address, 0.0.0.0, as the IP source address. And it doesn't know how to reach the DHCP server, so it uses a general broadcast address, 255.255.255.255, for the destination. So the router must replace the source address with its own IP address, for the interface that received the request. And it replaces the destination address with the address specified in the ip helper-address command. The client device's MAC address is included in the payload of the original DHCP request packet, so the router doesn't need to do anything to ensure that the server receives this information.

QUESTION 63
Refer to the exhibit. The network administrator made the entries that are shown and then saved the configuration. From a console connection, what password or password sequence is required for the administrator to access privileged mode on Router1?

```
Router# configure terminal
Router(config)# hostname Router1
Router1(config)# enable secret sanfran
Router1(config)# enable password cisco
Router1(config)# line vty 0 4
Router1(config-line)# password sanjose
Router1(config-line)#
```

A. cisco
B. sanfran
C. sanjose
D. either cisco or sanfran
E. either cisco or sanjose
F. sanjose and sanfran

Answer: B
Explanation:

The enable secret password takes precedence over the enable password, so sanfran will be used.

QUESTION 64
The following commands are entered on the router:
Burbank(config)# enable secret fortress
Burbank(config)# line con 0
Burbank(config-line)# login
Burbank(config-line)# password n0way1n
Burbank(config-line)# exit
Burbank(config)# service password-encryption
What is the purpose of the last command entered?

A. to require the user to enter an encrypted password during the login process
B. to prevent the vty, console, and enable passwords from being displayed in plain text in the configuration files
C. to encrypt the enable secret password
D. to provide login encryption services between hosts attached to the router

Answer: B

QUESTION 65
What is the effect of using the service password-encryption command?

A. Only the enable password will be encrypted.
B. Only the enable secret password will be encrypted.
C. Only passwords configured after the command has been entered will be encrypted.
D. It will encrypt the secret password and remove the enable secret password from the configuration.
E. It will encrypt all current and future passwords.

Answer: E
Explanation:
Encryption further adds a level of security to the system as anyone having access to the database of passwords cannot reverse the process of encryption to know the actual passwords which isn't the case if the passwords are stored simply.

QUESTION 66
An administrator has connected devices to a switch and, for security reasons, wants the dynamically learned MAC addresses from the address table added to the running configuration. What must be done to accomplish this?

A. Enable port security and use the keyword sticky.
B. Set the switchport mode to trunk and save the running configuration.
C. Use the switchport protected command to have the MAC addresses added to the configuration.
D. Use the no switchport port-security command to allow MAC addresses to be added to the configuration.

Answer: A
Explanation:
One can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts, hence enabling security as desired.

QUESTION 67
A company has placed a networked PC in a lobby so guests can have access to the corporate

directory. A security concern is that someone will disconnect the directory PC and re-connect their laptop computer and have access to the corporate network. For the port servicing the lobby, which three configuration steps should be performed on the switch to prevent this? (Choose three.)

A. Enable port security.
B. Create the port as a trunk port.
C. Create the port as an access port.
D. Create the port as a protected port.
E. Set the port security aging time to 0.
F. Statically assign the MAC address to the address table.
G. Configure the switch to discover new MAC addresses after a set time of inactivity.

Answer: ACF
Explanation:
If port security is enabled and the port is only designated as access port, and finally static MAC address is assigned, it ensures that even if a physical connection is done by taking out the directory PC and inserting personal laptop or device, the connection cannot be made to the corporate network, hence ensuring safety.

QUESTION 68
Why would a network administrator configure port security on a switch?

A. to prevent unauthorized Telnet access to a switch port
B. to prevent unauthorized hosts from accessing the LAN
C. to limit the number of Layer 2 broadcasts on a particular switch port
D. block unauthorized access to the switch management interfaces

Answer: B
Explanation:
You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port. If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

QUESTION 69
How can you ensure that only the MAC address of a server is allowed by switch port Fa0/1?

A. Configure port Fa0/1 to accept connections only from the static IP address of the server.
B. Configure the server MAC address as a static entry of port security.
C. Use a proprietary connector type on Fa0/1 that is incomputable with other host connectors.
D. Bind the IP address of the server to its MAC address on the switch to prevent other hosts from spoofing the server IP address.

Answer: B
Explanation:
When the MAC address is configured as static entry, no other address is allowed.

QUESTION 70

Interconnecting Cisco Networking Devices Part 1 (ICND1) (100-101)

Refer to the exhibit. A network administrator has configured a Catalyst 2950 switch for remote management by pasting into the console the configuration commands that are shown in the exhibit. However, a Telnet session cannot be successfully established from a remote host. What should be done to fix this problem?

```
interface vlan 1
ip address 192.168.17.253  255.255.255.240
no shutdown
exit
ip default-gateway 192.168.17.1
line vty 0 15
password cisco
login
exit
```

A. Change the first line to interface fastethernet 0/1.
B. Change the first line to interface vlan 0/1.
C. Change the fifth line to ip default-gateway 192.168.17.241.
D. Change the fifth line to ip route 0.0.0.0 0.0.0.0 192.168.17.1.
E. Change the sixth line to line con 0.

Answer: C
Explanation:
The default gateway for remote session is 192.168.17.241 and not the one given in the exhibit.

QUESTION 71
Which IP addresses are valid for hosts belonging to the 10.1.160.0/20 subnet? (Choose three.)

A. 10.1.168.0
B. 10.1.176.1
C. 10.1.174.255
D. 10.1.160.255
E. 10.1.160.0
F. 10.1.175.255

Answer: ACD
Explanation:
All IP address in IP ranges between : 10.1.160.1 and 10.1.175.254 are valid as shown below
Address: 10.1.160.0 00001010.00000001.1010 0000.00000000 Netmask:255.255.240.0 =
2011111111.11111111.1111   0000.00000000   Wildcard:0.0.15.25500000000.00000000.0000
1111.11111111 Which implies that
Network: 10.1.160.0/20   00001010.00000001.1010   0000.00000000
HostMin:10.1.160.100001010.00000001.1010   0000.00000001
HostMax:10.1.175.25400001010.00000001.1010   1111.11111110
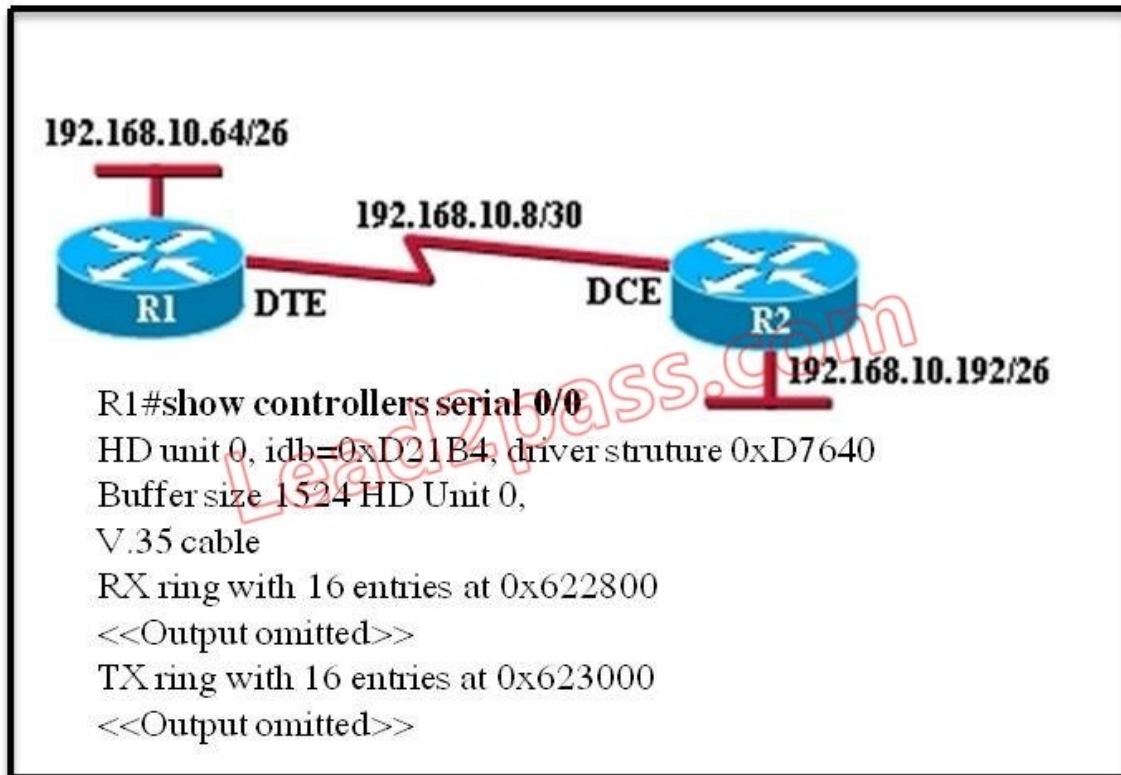Broadcast:10.1.175.25500001010.00000001.1010 1111.11111111

QUESTION 72
Refer to the exhibit. An administrator cannot connect from R1 to R2. To troubleshoot this problem, the administrator has entered the command shown in the exhibit. Based on the output shown, what could be the problem?

```
192.168.10.64/26

        192.168.10.8/30
R1  DTE              DCE
                          R2
                       192.168.10.192/26

R1#show controllers serial 0/0
HD unit 0, idb=0xD21B4, driver struture 0xD7640
Buffer size 1524 HD Unit 0,
V.35 cable
RX ring with 16 entries at 0x622800
<<Output omitted>>
TX ring with 16 entries at 0x623000
<<Output omitted>>
```

A. The serial interface is configured for half duplex.
B. The serial interface does not have a cable attached.
C. The serial interface has the wrong type of cable attached.
D. The serial interface is configured for the wrong frame size.
E. The serial interface has a full buffer.

Answer: C
Explanation:
since the output is not forthcoming it shows that the type of cable attached is wrong, though the cable is connected since it shows the cable type. According to the figure DTE cable should connect to R1 on interface but while examining using show controllers serial 0/0 command it showing that a DCE is connected so the wrong type of cable is being used.

QUESTION 73
Refer to the exhibit. A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has made a console connection to the NY router. After establishing the connection they are unable to backup the configuration file and IOS of the NY router to the TFTP server. What is the cause of this problem?

Interconnecting Cisco Networking Devices Part 1 (ICND1) (100-101)
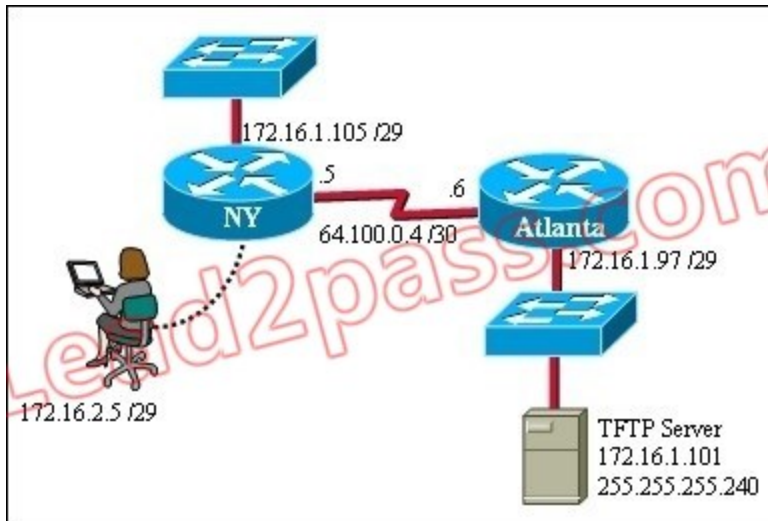
A. The NY router has an incorrect subnet mask.
B. The TFTP server has an incorrect IP address.
C. The TFTP server has an incorrect subnet mask.
D. The network administrator computer has an incorrect IP address.

Answer: C
Explanation:
The subnet mast of the TFTP server needs to be in tune with the other network requirements else it wont be possible.

QUESTION 74
If a host experiences intermittent issues that relate to congestion within a network while remaining connected, what could cause congestion on this LAN?

A. half-duplex operation
B. broadcast storms
C. network segmentation
D. multicasting

Answer: B
Explanation:
A broadcast storm can consume sufficient network resources so as to render the network unable to transport normal traffic.

QUESTION 75
Refer to the exhibit. The junior network support staff provided the diagram as a recommended configuration for the first phase of a four-phase network expansion project. The entire network expansion will have over 1000 users on 14 network segments and has been allocated this IP address space.
192.168.1.1 through 192.168.5.255
192.168.100.1 through 192.168.100.255
What are three problems with this design? (Choose three.)
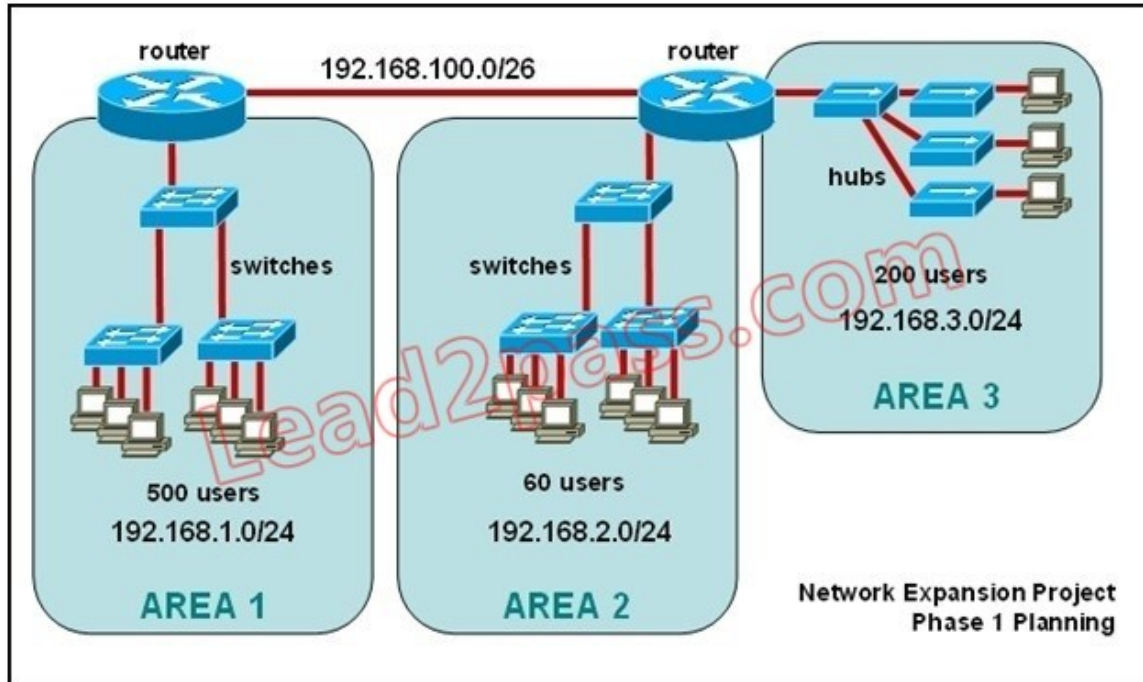
A. The AREA 1 IP address space is inadequate for the number of users.
B. The AREA 3 IP address space is inadequate for the number of users.
C. AREA 2 could use a mask of /25 to conserve IP address space.
D. The network address space that is provided requires a single network-wide mask.
E. The router-to-router connection is wasting address space.
F. The broadcast domain in AREA 1 is too large for IP to function.

Answer: ACE
Explanation:
The given IP addresses of areas 1 and 3 along with network masks of 24 cannot accommodate 500 users so are inadequate, while the area 2 is having over capacity so its network mask can be reduced to 25 to accommodate the only 60 users it has.

QUESTION 76
Given an IP address of 192.168.1.42 255.255.255.248, what is the subnet address?

A. 192.168.1.8/29
B. 192.168.1.32/27
C. 192.168.1.40/29
D. 192.168.1.16/28
E. 192.168.1.48/29

Answer: C
Explanation:
248 mask uses 5 bits (1111 1000)
42 IP in binary is (0010 1010)
The base subnet therefore is the lowest binary value that can be written without changing the output of an AND operation of the subnet mask and IP ...
1111 1000 AND
0010 1010 equals
0010 1000 - which is .40

/24 is standard class C mask.
adding the 5 bits from the .248 mask gives /29

QUESTION 77
Which OSI layer header contains the address of a destination host that is on another network?

A. application
B. session
C. transport
D. network
E. data link
F. physical

Answer: D
Explanation:
Only network address contains this information. To transmit the packets the sender uses network address and datalink address. But the layer 2 address represents just the address of the next hop device on the way to the sender. It is changed on each hop. Network address remains the same.

QUESTION 78
Which layer of the TCP/IP stack combines the OSI model physical and data link layers?

A. Internet layer
B. transport layer
C. application layer
D. network access layer

Answer: D
Explanation:
The Internet Protocol Suite, TCP/IP, is a suite of protocols used for communication over the internet. The TCP/IP model was created after the OSI 7 layer model for two major reasons. First, the foundation of the Internet was built using the TCP/IP suite and through the spread of the World Wide Web and Internet, TCP/IP has been preferred. Second, a project researched by the Department of Defense (DOD) consisted of creating the TCP/IP protocols. The DOD's goal was to bring international standards which could not be met by the OSI model. Since the DOD was the largest software consumer and they preferred the TCP/IP suite, most vendors used this model rather then the OSI. Below is a side by side comparison of the TCP/IP and OSI models.
TCP/IP Model
VS.
OSI Model Application Layer 7
Application
Layer 6
Presentation
Layer 5
Session Transport Layer 4
Transport Internet Layer 3
Network Network Access Layer 2
Data Link
Layer 1
Physical

QUESTION 79
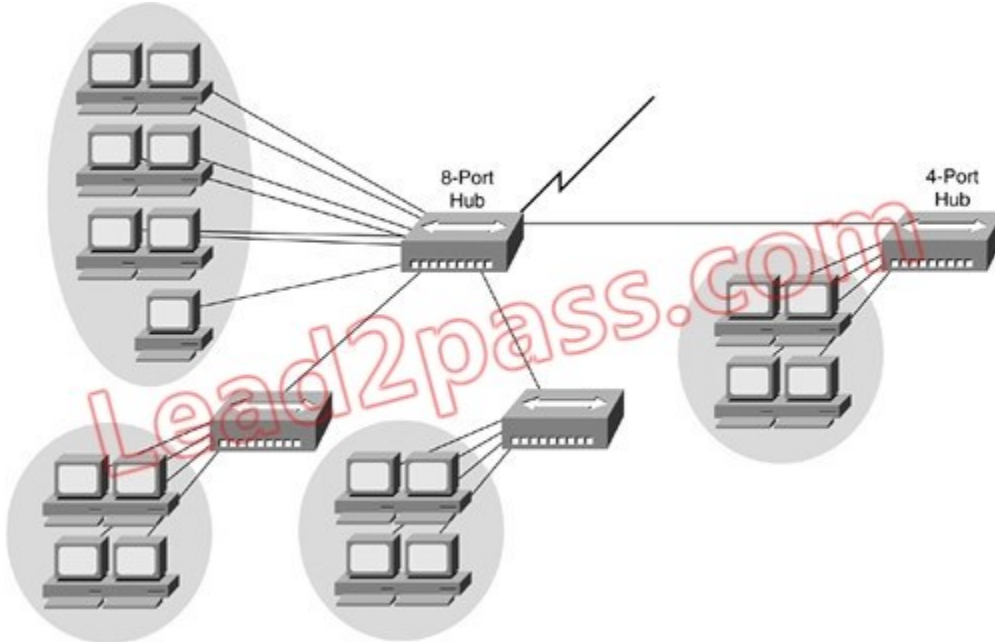Which protocol uses a connection-oriented service to deliver files between end systems?

A. TFTP
B. DNS
C. FTP
D. SNMP
E. RIP

Answer: C

QUESTION 80
Refer to the exhibit. If the hubs in the graphic were replaced by switches, what would be virtually eliminated?

A. broadcast domains
B. repeater domains
C. Ethernet collisions
D. signal amplification
E. Ethernet broadcasts

Answer: C
Explanation:
Modern wired networks use a network switch to eliminate collisions. By connecting each device directly to a port on the switch, either each port on a switch becomes its own collision domain (in the case of half duplex links) or the possibility of collisions is eliminated entirely in the case of full duplex links.